THE MSSP JOURNEY

A VISUAL GUIDE

Presented By

XENEX

and

Tech Data

Security Solutions

// For MSPs considering the transition to MSSP

Presented By
XENEX
and
Tech Data
Security Solutions

The Need for Cybersecurity

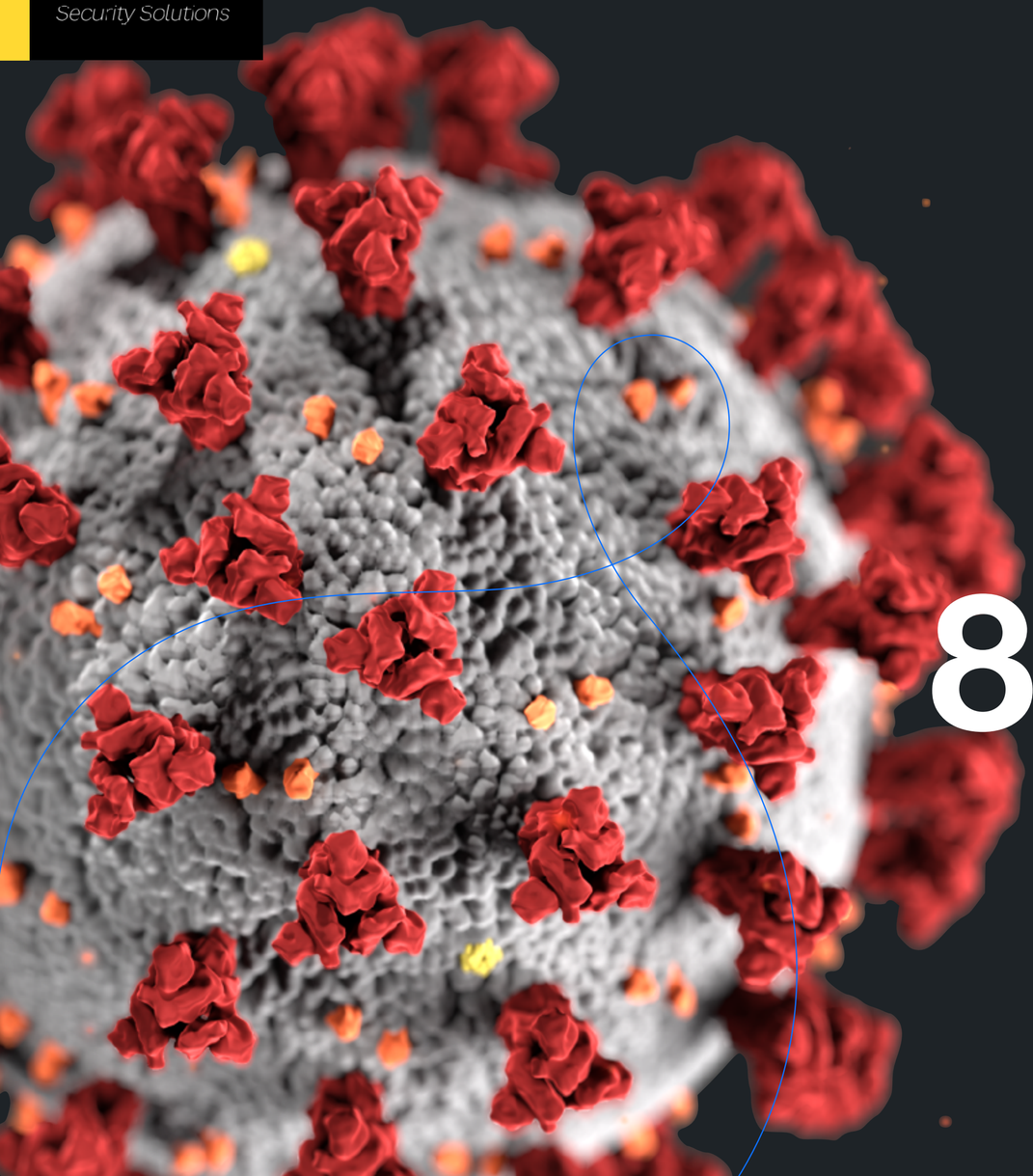
Demand is **increasing** for managed services to identify, investigate and respond to cybersecurity threats.

76%

Percentage of small and medium-sized businesses will experience **significant business disruption** as the result of a security breach in the next 36 months.

(Source: Kaseya Annual User Conference)

Presented By
XENEX
and
Tech Data
Security Solutions



COVID 19 Accelerating Challenges

Covid 19 triggered additional opportunities for bad actors to attack, across the board.

89%

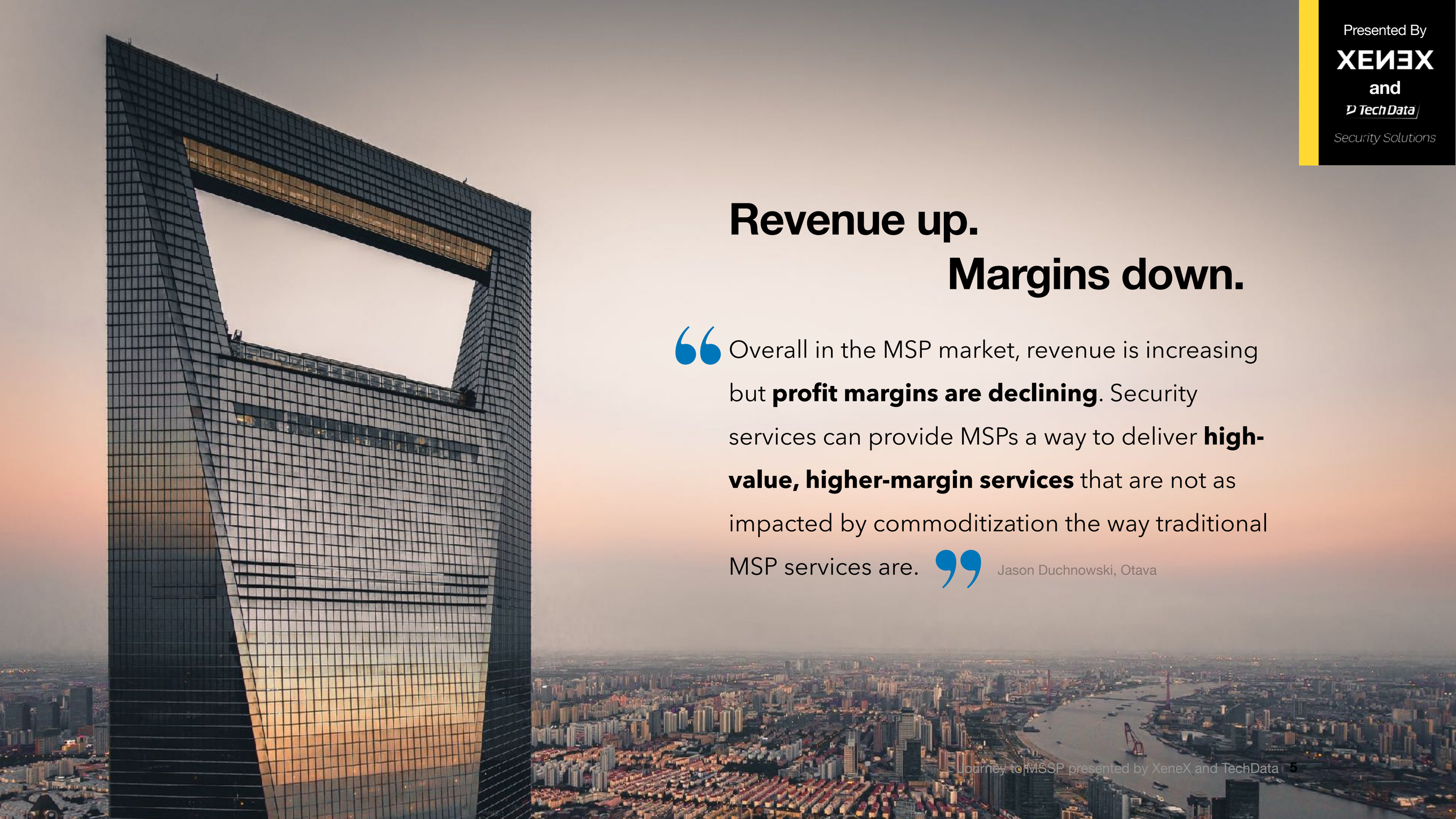
of MSPs cited ransomware as the most common threat to small and medium-sized businesses

(Source: Datto's Global State of the Channel Ransomware Report 2020)

17%

Of the 40,000 MSPs in North America are considered MSSPs.

Roughly 75% of MSPs that introduced security services into their repertoire experienced revenue increases within 12 months.



Presented By
XENEX
and
TechData
Security Solutions

Revenue up.
Margins down.

> Overall in the MSP market, revenue is increasing but **profit margins are declining**. Security services can provide MSPs a way to deliver **high-value, higher-margin services** that are not as impacted by commoditization the way traditional MSP services are.
>
> Jason Duchnowski, Otava

Presented By XENEX and TechData Security Solutions

The Opportunity

Being an MSSP presents some interesting opportunities for MSPs.

Customer Retention

According to a TechValidate survey, only 5% of MSSPs -vs- 87% of MSPs have lost business because they lacked security services needed by customers.

Growth

Structuring as an MSSP can bring financial and capability enhancement that increases opportunities and potential for growth.

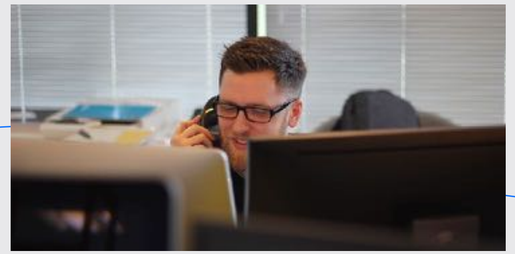
Survival

In addition to providing new opportunities, being increasingly focused on security also help protect the MSP itself from the increasing myriad security risks it faces.

Retention & MRR

MSPs experience an average churn rate of 75% in North America. By contrast, MSSPs experience greater customer retention and monthly recurring revenues.

…But it's not all upside.



Talent

MSSPs deal with sensitive and mission critical technologies and techniques that require a highly specialized and talented labor pool.

Complexity

Security is a 24/7 very complex process involving integrations and workflows that protect against increasingly sophisticated attackers. There is no room for error.

Liability & Compliance

MSSPs are exposed to data sovereignty, protection and privacy liability issues around numerous regulatory and compliance requirements that often require extra insurances.

Becoming an MSSP is a huge opportunity, but is also very expensive.

Presented By
XENEX
and
Tech Data
Security Solutions

Breaking down the costs.

Risky. Complex. Expensive.

Technology

Upfront hardware and software costs and providing unlimited cloud-based DDoS protection can be prohibitively expensive.

Operations

MSSPs are expected to run Security Operations Centers that provide 24x7x365 security and support. We'll take a closer look at what goes into this later in this guide.

Maintenance

Maintenance costs for appliances/hardware also need to be considered.

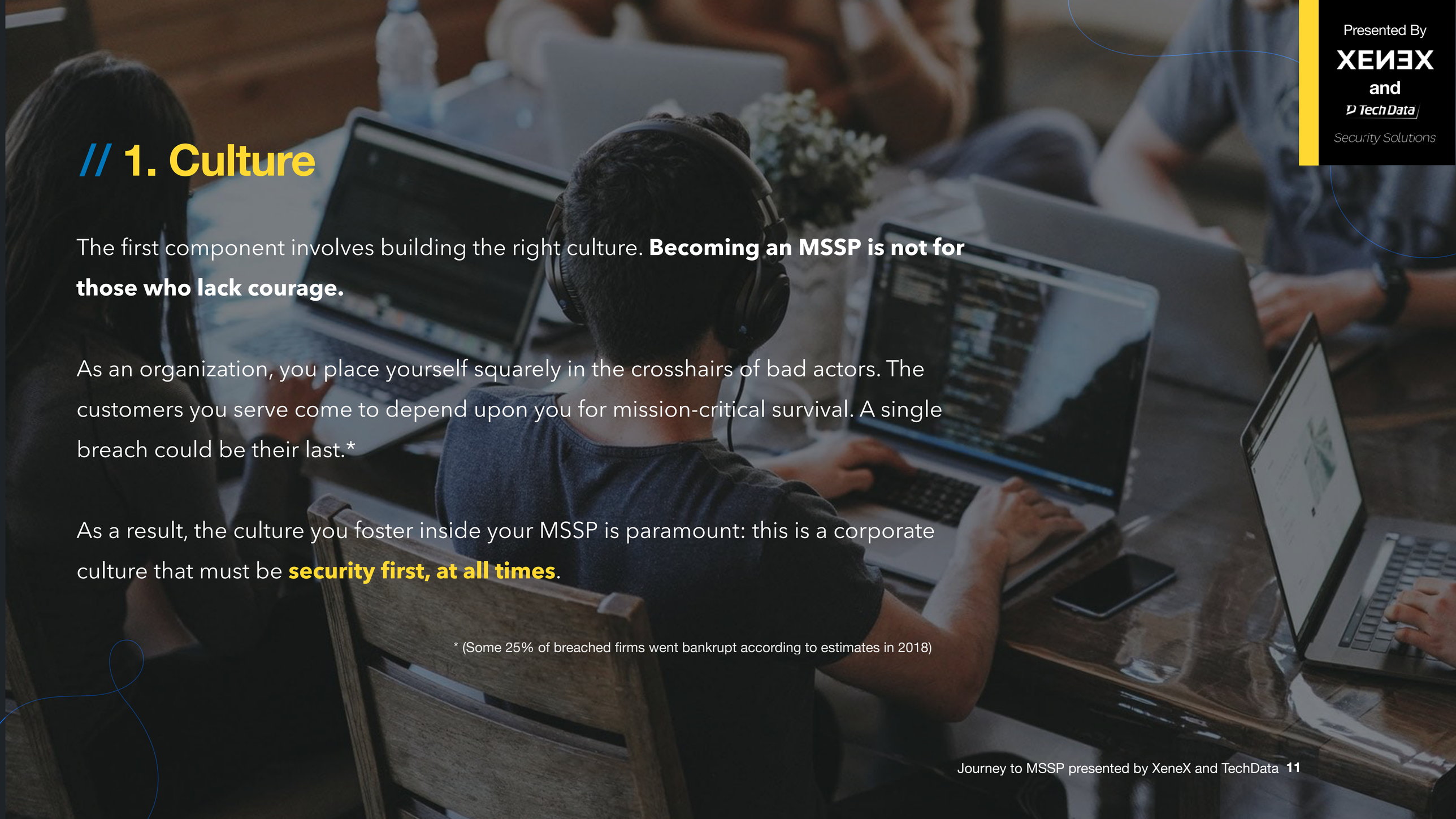
Marketing

In addition to expected marketing and advertising costs, launch will require talented teams, including expensive cybersecurity professionals as well as sales, support and other roles.

> We know this will be a challenge and we are ready to meet that challenge. — **You**

Now that you've decided to embark on this great adventure, let's examine some of the key components you're going to need to put together to be successful.

Presented By XENEX and TechData Security Solutions



Presented By XENEX and TechData Security Solutions

// 1. Culture

The first component involves building the right culture. **Becoming an MSSP is not for those who lack courage.**

As an organization, you place yourself squarely in the crosshairs of bad actors. The customers you serve come to depend upon you for mission-critical survival. A single breach could be their last.*

As a result, the culture you foster inside your MSSP is paramount: this is a corporate culture that must be **security first, at all times**.

* (Some 25% of breached firms went bankrupt according to estimates in 2018)

// 2. Process

Next, defining processes inside the organization that support the **security first** culture while adhering to **legal and regulatory compliance** is key. Processes directly related to delivered services, as well as more general activities such as screening an hiring are all critical to a successful operation.

It may be tempting to move quickly towards specific technologies or solutions, but in all cases, it is far more advisable to begin with a well-defined process/workflow strategy and operational framework to which particular technologies and personnel are matched.

// 3. People

Building the right team is essential.

From the security team to the internal sales and marketing team, everyone is involved in supporting culture of security and executing on processes that reduce risk while increasing efficiency and driving innovation.

Go deep into backgrounds, holding multiple interviews across departments. Involve technology experts in screening. Conduct appropriate background checks. Likely, salaries in this industry will be higher than many others. Don’t skimp on finding and compensating the right talent. Given the sensitive nature of the business MSSPs are in, every person hired (from CTO to intern) can be an extraordinary asset or a dangerous liability.

// 4. Technology

In addition to a wide range of technologies, an MSSP must be able to deliver a Security Operations Center (SOC) with both the latest physical and logical security technologies. Because an MSSP focuses on security, in addition to standard IT functions it typically provides many, if not all of the following:

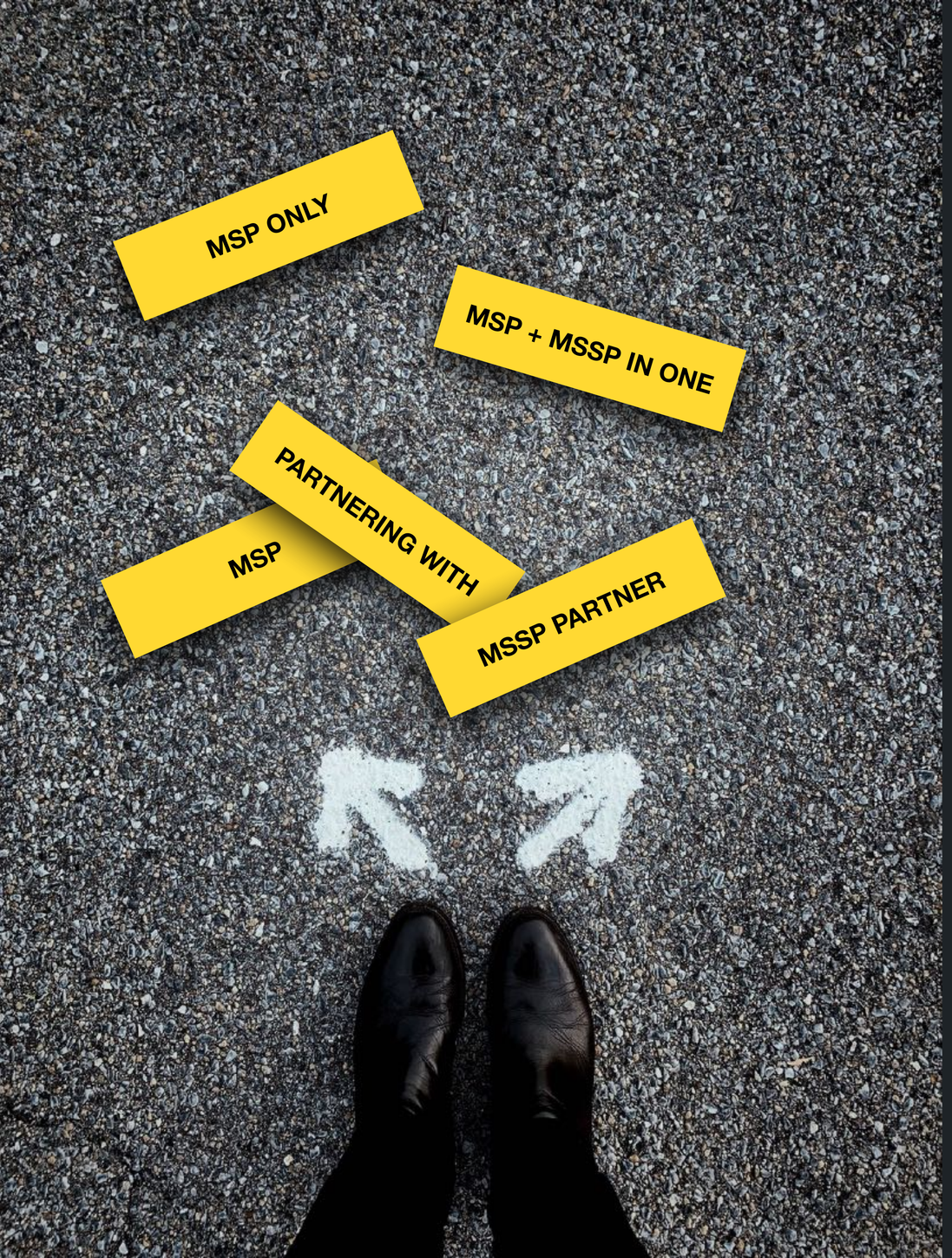
- A technology suite to manage a customer's IT and infrastructure with remote helpdesk
- Security operations capabilities with shared remote services from a remote SOC
- Remote 24/7 monitoring of security events and data sources
- Endpoint security / endpoint detection and response
- Breach detection
- Enforced security policies
- Patch management
- Security information event management (SIEM)

// 5. Partnering

The requirements for establishing a proper SOC are enormous. Not only must a company fortify itself with proper physical security, but it must prepare for any digital security eventuality (whether from external sources or even internal). The requirements for trained and skilled cybersecurity staff can be even more daunting, given the present labor market. Finally, carrying the correct legal and business coverages (insurances) adds an extra element of challenge.

Because of these reasons and others, teaming up with a partner may represent a more sensible (and economical) approach. With the proper implementation of a partnership (with technologies, training and automation in place) may also represent a significant strategic advantage as well.

We'll explore this in the next section.



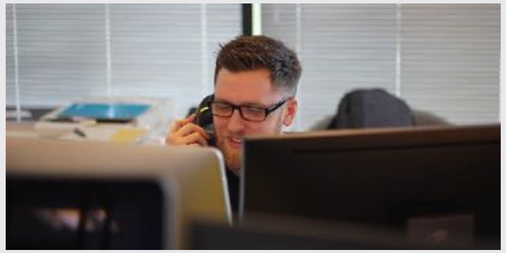
Presented By
XENEX
and
TechData
Security Solutions

DIY -vs- Partnering

As an MSP looking to transition to becoming an MSSP, it may be tempting to forge ahead and “do it all” under one umbrella, integrating the core functions of an MSP and MSSP under one roof.

However, there are major drawbacks to this you may want to consider.

Potential Conflicts

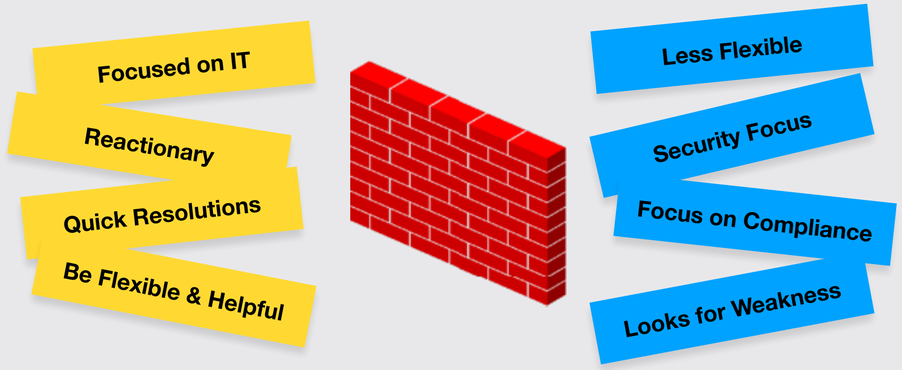


Consider a Business Firewall

Blending both MSP and MSSP roles into a single function poses serious potential conflicts as it reduces the natural checks and balances that exist between two very different focuses.

MSP

Provide technology and processes to manage a customer's IT infrastructure with some remote helpdesk support. Lacks a true SOC and isn't specialized in cybersecurity, where often times security is secondary to immediate IT needs.



MSSP

Focuses on cybersecurity and delivers Security Operations Center (SOC) that provides 24x7x365 security and support with remote helpdesk. Some MSSPs provide remediation services in case of attack.

Keeping each function separate and accountable provides the best potential outcome.

Partner with Us

Since 2011 XeneX has been a pioneer in developing a single platform to correlate security insights with monitoring data across infrastructure, network and application tiers. You get the visibility you need to understand and respond to potential threats faster and more accurately.

XeneX Endpoint Protection, together with Security Monitoring platform, XeneX XDR (cross correlation engine), and out-of-the-box seamless integration with virtually any source of security data enables a more holistic and, ultimately, a more robust approach to security, without increasing the operational burden of deploying and maintaining multiple, disconnected point solutions.

If your organization decides to partner with a Security Operations Center (SOC) partner with a deep technology and security bench with available 24/7/365 monitoring, give us a call at (877) 550 2568 or email us at sales@xenexsoc.com.

www.xenexsoc.com